

DA PRIVACY IMPACT ASSESSMENT (PIA)

1. DA organizational name (APMS Sub Organization name)

U.S. Army Corps of Engineers (USACE)

2. Name of Information Technology (IT) System (APMS System name)

Resident Management System (RMS)

3. Budget System Identification Number (SNAP-IT Initiative Number)

9997

4. System Identification Number(s) (IT Registry/Defense IT Portfolio Repository (DITPR/Army AITR)).

3835

5. IT Investment (OMB Circular A11) Unique Identifier (if applicable).

202-00-01-02-01-1032-00-301-093

6. Privacy Act System of Records Notice Identifier (if applicable).

N/A

7. OMB Information Collection Requirement Number (if applicable) and expiration date.

N/A

8. Type of Authority to collect information (statutory or otherwise).

P.L. 403-74, S.3303, Davis Bacon Act
Engineer Regulation (ER) 1180-1-8 Contracts: Labor Relations

9. Provide a brief summary or overview of the IT system.

Resident Management System (RMS) is a corporate, automated information system used by USACE employees and contractors involved with the construction phase of a project. It is used mainly for construction quality assurance management and contract administration, and helps to standardize construction business practices throughout the command. It also serves as a multi-purpose administration and automation tool for construction field offices. This component provides an efficient method to plan, accomplish, and maintain control over of construction projects.

DA PRIVACY IMPACT ASSESSMENT (PIA)

The RMS Quality Control System (QCS) module provides a systematic approach to various labor standards compliance activities. Among the activities addressed in the Quality Assurance/Quality Control (QA/QC) planning phase is to plan and track labor standards interviews and contractor payroll submissions. The QA/QC module assists in the investigation of labor standards complaints alleging contractor non-compliance with contract labor provisions.

10. Describe what information in identifiable form will be collected and the nature and source of the information.

Information is manually collected on a Standard Forms (SF) 1445 Labor Standards Interview form. Selected data from the SF1445 is keyed into RMS including, Employer name, Employee name, Employee Address, Employee Work [Labor] Classification, Required Labor Rate (RLR), and Paid Labor Rate (PLR). After data entry in RMS, the completed SF114 is attached to the Contractor's certified payroll and forwarded to the local USACE Labor Office.

11. Describe how the information will be collected.

The USACE Quality Assurance Representative provides a SF1445 Labor Standards Interview form to Contractor employees on a random basis. The employee is advised that pursuant to the Privacy Act (5 USC 552a) the information being furnished is confidential and that their identity will not be disclosed to the employer without the employee's consent. A Privacy Act Statement is also attached to the SF1445. The Contractor employee manually completes and signs the form and returns it to the USACE QA Representative for processing (see #10 above). Labor Standards Interviews are generally conducted on a weekly basis.

12. Describe the requirement and why the information in identifiable form is to be collected.

The information is collected to ensure compliance with the wage provisions of the Davis Bacon Act, to ensure workers are paid the appropriate wage based on geographical area.

13. Describe how the information in identifiable form will be used.

The Required Labor Rate (RLR) is compared to the Paid Labor Rate (PLR). If the PLR is less than the RLR, the employee entry is flagged in RMS under Labor Interviews and the local USACE Labor Office is notified. Alleged contractor non-compliance with contract labor provisions are referred by the USACE Labor Office to local USACE Counsel for resolution.

14. Describe whether the system derives or creates new data about individuals through aggregation.

DA PRIVACY IMPACT ASSESSMENT (PIA)

This system does not create new data about individuals through aggregation

15. Describe with whom the information in identifiable form will be shared, both within DA and outside DA.

USACE District Area/Resident Office personnel that have a need to know in order to perform official duties and the local RMS Data Base Administrator have access to the information.

Internal DoD agencies that would obtain access to PII in this system, on request in support of an authorized investigation or audit, may include DOD IG, DCIS, Army Staff Principals in the chain of command, DAIG, AAA, USACIDC, INSCOM, PMG and ASA FM&C. In addition, the DoD blanket routine uses apply to this system. ...

16. Describe any opportunities individuals will have to object to the collection of information in identifiable form about themselves or to consent to the specific uses of the information in identifiable form.

According to policy, the employee is advised that pursuant to the Privacy Act (5 USC 552a) the information being furnished is confidential and that their identity will not be disclosed to the employer without the employee's consent.

17. Describe the process regarding how the individual is to grant consent.

USACE QA Representatives use SF Form 1445 Labor Standards Interview when conducting interviews. These interview reports are used as a check against the contractor's or subcontractor's payroll for the week

18. Describe any information that is provided to an individual and the format of such information and means of delivery.

A separate format containing Privacy Act advisories is reproduced locally and attached to the SF Form 1445.

19. Describe the administrative/business, physical, and technical processes and controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form.

This system has a current certification and accreditation. The system resides on a secure military installation within secured facilities.

DA PRIVACY IMPACT ASSESSMENT (PIA)

The data is stored within a secure datacenter on a secure Army facility with all protections afforded by Army and Defense Information System Agency (DISA) security infrastructure. The datacenter has passed the required security measures tests required for Information Assurance System Accreditation and has a full Authority to Operate. Additionally, the system is built on redundancy with a full Continuity of Operations (COOP) site.

All aspects of privacy, security, configuration, operations, data retention and disposal in regards to information in identifiable form are documented in policies to ensure that privacy and security are consistently enforced and maintained. The impact of loss was evaluated for the information in identifiable form and is protected accordingly. A user's manual was designed to fulfill the needs of the different types of employees (e.g., users, administrators, managers, security officers) who will use the system. This system has a comprehensive security system that controls access to records. Access can be granted on an individual or group basis. The confidentiality of all data is protected by measures appropriate for unclassified system high operations with "need-to-know controls". All users are appropriately cleared for privileges based on individual user job requirements. Privileges are limited to only those necessary for job requirements.

20. Identify whether the IT system or collection of information will require a System of Records notice. If not published, state when publication of the notice will occur.

N/A. Purpose of RMS is not to retrieve PII by individuals' names or other personal identifiers.

21. Describe/evaluate any potential privacy risks the collection, use, and sharing of the information in identifiable form.

Due to the level of safeguarding, we believe the risk to individuals' privacy to be minimal. There are no risks in providing an individual the opportunity to object or consent, or in notifying individuals. Risk is mitigated by consolidation and linkage of files and systems, derivation of data, accelerated information processing and decision making, and use of new technologies.

22. Describe/evaluate any privacy risks in providing individuals an opportunity to object/consent or in notifying individuals.

There are no risks in providing an individual the opportunity to object or consent, or in notifying individuals.

23. Describe/evaluate any risks posed by the adopted security measures.

Due to the level of safeguarding, we believe the risk to individuals' privacy to be minimal.

DA PRIVACY IMPACT ASSESSMENT (PIA)

24. State classification of information/system and whether the PIA should be published or not. If not, provide rationale.

Unclassified For Official Use Only.

25. If a PIA is planned for publication, state whether it will be published in full or summary form.

The PIA may be published in its entirety.